

EXHIBIT D

**IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT**

AL OTRO LADO, INC., *et al*
Plaintiffs-Appellees,

v.

ALEJANDRO MAYORKAS, *et al.*,
Defendants-Appellants.

No. 19-56417

D.C. No. 3:17-cv-02366-BAS-KSC
Southern District of California,
San Diego

DECLARATION OF JOHN BUCKLEY

I, John Buckley, pursuant to 28 U.S.C. § 1746, and based upon my personal knowledge and information made known to me from official records and reasonably relied upon in the course of my employment, hereby declare as follows, relating to the above-captioned matter:

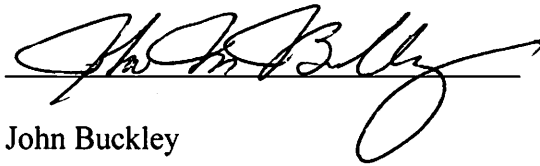
1. I am currently the Director, Security and Technology Division, Office of Information Technology, U.S. Customs and Border Protection (CBP). As the Director of the Security and Technology Division, I am responsible for ensuring that CBP's information technology (IT) systems comply with policies established by the Department of Homeland Security, the Office of Management and Budget, and the National Institute of Standards and Technology. I manage the staff who are responsible for creating CBP's IT security policies, security awareness trainings, independent security tests and evaluations, and certification and accreditation programs.
2. I understand that the Court denied the parties' Motion to Seal on or about November 21, 2019. I also understand that the defendants requested, in part, to seal certain information relating to the personal telephone numbers and the email addresses of senior CBP officials.

3. Disseminating the email addresses of CBP employees without sufficient protection can create significant cyber security threats to both the individual employee and CBP as a whole.
4. Once an employee's email address is publicized, malicious actors can engage in social engineering to obtain confidential information from that employee. Social engineering is the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes. Types of social engineering include:
 - a. Phishing: the practice of sending emails purporting to be from reputable sources with the goal of influencing or gaining personal information such as passwords or financial information.
 - b. Spear phishing: a type of highly targeted phishing attack that focuses on a specific individual or organization.
5. There are a number of other cyber security threats that can occur once an employee's email address is released to the public. These threats include:
 - a. A denial of service (DoS) attack: a DoS is a security event that happens when an attacker prevents legitimate users from accessing specific computer systems, devices, services or other IT resources. The purpose of a DoS is to flood servers, systems, or networks with traffic to overwhelm the victim's resources and make it difficult or impossible for legitimate users to access them.
 - b. Doxing: doxing occurs when a malicious actor publishes private personal information, usually for the purposes of public humiliation, stalking, identity theft, or targeting an individual for harassment.

- c. Swatting: swatting is a harassment tactic in which a malicious actor deceives emergency services into sending police or emergency response teams to another person's address.
 - d. Ransomware: ransomware is malicious software designed to block access to a computer system until a sum of money is paid.
 - e. Spam email or "spamming:" spamming occurs when disruptive online messages are sent repeatedly. Spam emails make hinder an agency's ability to communicate with its employees due to the volume of email traffic and strains on the agency's IT capacities.
6. Cyber attacks against the U.S. Government are on the rise. A report by the Government Accountability Office found that between 2006 and 2015, cyberattacks involving systems supporting the federal government increased over 1,300% from 5,500 to over 77,000. *See* GAO-16-501, Information Security: Agencies Need to Improve Controls over Selected High-Impact Systems (May 2016).
7. The Office of Personnel Management discovered that it was the victim of a cyber attack in April 2015. Hackers stole personal information belonging to 21.5 million federal employees and their families, friends, and former employers. The hackers were able to compromise the entire OPM network by exploiting the credentials of one single contractor.
8. Publication of CBP employees' email addresses therefore poses a substantial risk to the safety and welfare of the individual employee and CBP. For these reasons, any documents in this case that contain such information should be filed under seal and kept confidential. Alternatively, the Court should permit Defendants to redact email addresses before the underlying documents are publicly released.

9. I declare, under penalty of perjury, that the foregoing is true and correct to the best of my knowledge, information, and belief.

Executed this 11 day of February, 2020.

A handwritten signature in black ink, appearing to read "John Buckley", is written over a horizontal line.

John Buckley

Director, Security and Technology Division

Office of Information Technology

U.S. Customs and Border Protection